UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

mw

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,006	09/28/2001	David J. Lineman	12225.0035.NPUS00	4813

20792 7590 10/19/2006

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/966,006
Filing Date: September 28, 2001
Appellant(s): LINEMAN ET AL.

Robert W. Glatz
Reg. No. 36,811
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed July 13, 2006 appealing from the Office action mailed December 13, 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

No evidence is relied upon by the examiner in the rejection of the claims under appeal.

6,735,701	JACOBSON	05-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-56 are rejected under 35 U.S.C. 102(e) as being anticipated by Jacobson, U.S. Patent 6,735,701.

As per claim 1, it is disclosed by Jacobson of a method for managing a security policy for users in a network. A policy management program is run on a computer in communication with the network for enabling creation of a security policy document in a portable representation language using the policy management program that includes selection and inclusion in the security policy document of data elements for communicating the security policy to a user and a data element for implementing the security policy on computer systems in the network. Users on the network are enabled to view the security policy document using the plurality of data elements for communicating the security policy to users included in the security policy document and receiving electronic data relevant to user viewing of the security policy document using the policy management program (col. 2, lines 3-18; col. 10, line 57 through col. 11, line 3; and col. 19, lines 19-32).

As per claims 2 and 31, Jacobson discloses of verifying a degree of user compliance with the security policy by using the policy management program to assess the received data (col. 11, lines 3-9).

As per claim 3, Jacobson discloses of the received data includes a timestamp denoting the time a user acknowledges viewing of the security policy document (col. 20, lines 39-55).

As per claims 4 and 32, it is taught by Jacobson of the received data includes quiz results Indicative of the user comprehension of the viewed security policy document (col. 5, lines 37-40 and col. 6, lines 48-60).

As per claims 5 and 33, the teachings of Jacobson disclose of enabling the creation of the security policy document comprises enabling selection of security policies from a set of options (col. 6, lines 47-57).

As per claims 6,12, and 34, Jacobson discloses of selecting the security policies selected a set of options reside in a library in communication with the policy management program (col. 20, lines 24-26).

As per claim 7, it is taught by Jacobson of enabling the users on the network to view the security policy document comprises enabling pre-selection of a group of users to view the security policy document (col. 5, lines 51-65).

As per claims 8 and 36, Jacobson discloses of comprising electronically providing a quiz to assess user comprehension of the viewed security policy document (col. 5, lines 37-40 and col. 6, lines 48-60).

As per claim 9, Jacobson teaches of enabling the creation of the security policy document further comprises enabling creation of a quiz associated with the security policy document (col. 5, lines 37-40 and col. 6, lines 48-60).

As per claim 10, it is disclosed by Jacobson of receiving data includes user responses to the quiz (col. 5, lines 37-40 and col. 6, lines 48-60).

As per claim 11, Jacobson teaches of a method for managing a security policy for computers in a network. A software program is run on a second computer in communication with the network that enables the creation of a security policy document using the software program by enabling selection of security policies from a set of options. Automatically configuring the security policy document to provide technical controls for implementing the security policy on at a first computer (col. 2, lines 3-18; col. 10, line 57 through col. 11, line 3; and col. 6, lines 47-57).

As per claims 13 and 46, Jacobson discloses that the computers operate in accordance with different operating systems (col. 1, lines 60-63 and col. 5, lines 2-7).

As per claims 14 and 47, it is taught by Jacobson that the technical controls comprise a format interpretable by at least one first computer (col. 1, lines 60-63 and col. 5, lines 2-7).

As per claims 15 and 48, Jacobson discloses that the security policy document is represented by a markup language (col. 5, lines 2-7).

As per claims 16 and 49, Jacobson teaches of distributing detect rules to a first computer (col. 8, lines 7-10).

As per claims 17 and 50, it is disclosed by Jacobson of electronically notifying an administrator when at least one first computer is out of compliance (col. 18, lines 52-54).

As per claim 18, Jacobson discloses of distributing technical controls to at least one first computer (col. 2, lines 14-19).

As per claim 19, it is taught by Jacobson of running a second software program on the first computer to allow at least one first computer to interpret the distributed technical controls (col. 2, lines 14-19).

As per claims 20 and 40, Jacobson discloses of a second software program uses metacommands to convert the technical controls into instructions interpretable by an operating system running on the first computer (col. 1, lines 60-63 and col. 5, lines 2-7).

As per claims 21 and 41, Jacobson teaches of receiving data relevant to compliance of the first computer with the one or more technical controls using the software program (col. 2, lines 14-19).

As per claims 22 and 42, it is disclosed by Jacobson of further comprising assessing the received data using a third software program (col. 2, lines 14-19).

As per claims 23 and 43, it is taught by Jacobson that the third software program comprises a security management program (col. 2, lines 14-19).

As per claims 24 and 44, Jacobson discloses of verifying a degree of compliance of the first computer with the one or more technical controls by using the software program to assess the received data (col. 5, lines 37-40 and col. 8, lines 48-60).

As per claims 25 and 45, Jacobson teaches that the received data comprises compliance score data (col. 5, lines 37-40 and col. 8, lines 48-60).

As per claim 26, Jacobson discloses of a method for managing a security policy for users and computers in a network. A software program is run on a second computer in communication with the network. A security policy document is created using the software program and automatically configuring the security policy document to create human-readable security policy document and a machine-readable security policy document containing technical controls readable by the first computer (col. 2, lines 3-18; col. 10, line 57 through col. 11, line 3; and col. 6, lines 47-57).

As per claim 27, it is taught by Jacobson of allowing the users to view the human-readable security policy document via the network (col. 5, lines 51-65).

As per claim 28, Jacobson discloses of allowing the users to view the human-readable security policy document comprises pre-selecting a group of users to view the security policy document (col. 5, lines 51-65).

As per claim 29, Jacobson teaches of electronically receiving data relevant to user viewing of the security policy document (col. 5, lines 37-40 and col. 6, lines 48-60).

As per claim 30, Jacobson discloses that the received data includes a timestamp denoting the time a user acknowledged viewing the security policy (col. 20, lines 39-55).

As per claim 35, it is taught by Jacobson that the human-readable security policy document includes a quiz to test user comprehension of the security policy document (col. 5, lines 37-40 and col. 6, lines 48-60).

As per claim 38, Jacobson discloses of distributing the machine-readable security policy document to at least one first computer to implement the security technical controls thereon (col. 1, lines 60-63 and col. 5, lines 2-7).

As per claim 39, it is taught by Jacobson of running a second software program on the first computer to allow at least one first computer to interpret the distributed technical controls (col. 2, lines 14-19).

As per claim 51, Jacobson discloses of a system for managing a security policy for users and computers in a network. A first device containing a first program for creating a security policy document in both human-readable and machine-readable formats. A second device in communication with the first device and containing a second program for monitoring the security compliance of the first computer, wherein at least one first computer contains a third program for receiving the machine-readable format of the security policy document (col. 2, lines 3-18; col. 10, line 57 through col. 11, line 3; and col. 6, lines 47-57).

As per claim 52, Jacobson teaches that the portable representation language comprises a structured data representation language (col. 19, lines 19-32).

As per claim 53, it is disclosed by Jacobson that the plurality of data elements for communicating the security policy to users includes a policy statement element, a policy commentary element, and an example element wherein the data element for implementing the security policy on computer systems in the network includes a platform control element specific to a platform type corresponding to an operating system of one of the computer systems (col. 1, lines 11-16 and col. 19, lines 19-32).

As per claim 54, Jacobson teaches of enabling creation of the security policy document comprising enabling creation of a plurality of security policy documents associated with the security policy, one of the security policy documents includes data elements for different platform types corresponding to operating systems of the computer systems in the network (col. 1, lines 11-16 and col. 19, lines 19-32).

As per claim 55, Jacobson discloses that one of the computers in the network comprise a plurality of first computers, one of which are different platform types corresponding to operating systems of the respective first computers, the method further includes a plurality of platform controls, ones of which include commands for enforcing the security policy on the different platform types corresponding to operating systems of the plurality of first computers in the network (col. 1, lines 11-16 and col. 19, lines 19-32).

As per claim 56, the teachings of Jacobson disclose that one of the first computers in the network comprises a plurality of first computers, ones of which are different platform types corresponding to operating systems of the respective first computers and wherein enabling creation of a security policy document comprises creation of a plurality of security policy documents associated with the security policy, the method further includes a platform control that includes commands for enforcing the security policy on a corresponding one of the different platform types (col. 1, lines 11-16 and col. 19, lines 19-32).

(10) Response to Argument

Claim 1

It is argued by the Appellant that the teachings of Apperson fail to disclose of *distinct data elements for implementing the security policy on a computer.* The Appellant then points to the Appellant's specification for examples at paragraph 47 which recites "the platform controls that link the written security policy to the mechanism for communicating the security policy to the computer systems 26 on the various platforms" and "the technical controls that link the written policy to the mechanism for enforcing the security policy on the computer systems." Such data elements are not discussed by the teachings of Jacobson.

The examiner respectfully disagrees with the Appellant's assertion. The *distinct data elements for implementing the security policy on a computer*, specifically, the data element is vague as to what constitutes a "data element" in the claim language, and there is no language in the claim to further limit the terminology of a "data element".

The examiner is broadly interpreting the "data element" as being just a software program. Jacobson discloses that hardware implements the policy effectiveness system, or data element as claimed by the Appellant, that includes computers having processors and memories, see column 4, lines 65-67. It is further disclosed by Jacobson that the network communications software programs, or data elements, are used for policy effectiveness and reporting, see column 1, lines 60-63. Jacobson further discloses of block 500 represents the software compliance module of the policy effectiveness system 100, or data element, see column and as shown in Figure 5. The teachings of Jacobson do indeed disclose of *distinct data elements for implementing the security policy on a computer.*

The examiner is not giving weight to the term "data element" as being "the platform controls that link the written security policy to the mechanism for communicating the security policy to the computer systems 26 on the various platforms" and "the technical controls that link the written policy to the mechanism for enforcing the security policy on the computer systems" since these are features that which are not claimed. In response to Appellant's argument that the references fail to show certain features of Appellant's invention, it is noted that the features upon which Appellant relies (i.e., "the platform controls that link the written security policy to the mechanism for communicating the security policy to the computer systems 26 on the various platforms" and "the technical controls that link the written policy to the mechanism for enforcing the security policy on the computer systems.") are not recited in the rejected claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The Appellant argues that Jacobson fails to disclose of a *security policy document*. It is argued by the Appellant that an HTML type provision of information to remote locations executing on a browser is inferred in Jacobson, it does not follow that the HTML would disclose or suggest the "security policy document" that include HTML form information. It is asserted that Jacobson displays may be standard pages or frame displays saved on a system, text information stored in a database and extracted by the policy training module and/or various known other ways to create HTML pages or the like.

The examiner respectfully disagrees with the applicant's assertion. The claimed *security policy document"* is vague as to what constitutes a "security policy document" in the claim language, and there is no language in the claim to further limit the terminology of a "security policy document". It appears that the Appellant is relying upon examples from the specification as to what constitutes a "security policy document" and those elements are not recited in the claim. The teachings of Jacobson disclose of accessing the policy training materials through use of a hypertext list of policy training options that include policy training sessions, review for a policy exam, and taking a policy exam, see column 5, line 66 through column 6, line 4. The presentation through hypertext links is interpreted as the documents that include specific security documents such as policy training sessions, review for a policy exam, and taking a policy exam as is disclosed by Jacobson. The examiner notes that the

Appellant is arguing Jacobson fails to disclose of the *security policy document* does not contain HTML form information and the claim does not mention any use of HTML, but rather recite of a portable representation language which the examiner is equating to the document being received via hyperlinks. In response to Appellant's argument that the references fail to show certain features of Appellant's invention, it is noted that the features upon which Appellant relies (i.e., HTML) are not recited in the rejected claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). It appears that the Appellant is asserting what the *security policy document* isn't in view of the teachings of Jacobson and the Appellant has failed to address what the *security policy document* is according to the Appellant's invention.

The Appellant argues that the examiner does not distinguish between the recited *policy management program* and the recited *policy document* of claim 1 and Jacobson fails to disclose of enabling *creation* of such stored policies.

The examiner disagrees with the Appellant's assertion, the arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Jacobson discloses that of a policy training module 105, or policy management program, that is responsible for the handling the policy effectiveness system 100, see column 5, lines 36-65 and as shown in Figure 1. The claimed *security policy document"* is vague as to what constitutes a "security policy document" in the claim language, and there is no language in the claim to further limit the terminology of a "security policy document". It appears that the Appellant is relying upon examples from the specification as to what constitutes a "security policy document" and those elements are not recited in the claim. The teachings of Jacobson disclose of accessing the policy training materials through use of a hypertext list of policy training options that include policy training sessions, review for a policy exam, and taking a policy exam, see column 5, line 66 through column 6, line 4. The presentation through hypertext links is interpreted as the documents that include specific security documents such as policy training sessions, review for a policy exam, and taking a policy exam as is disclosed by Jacobson. Jacobson further discloses that the network policies are generated, or created, by guidelines created from employee feedback obtained during a training session, see column 5, lines 48-50. Block 220 represents a policy training module 105 generating a policy, see column 7, lines 61-62 and as shown in Figure 2.

The examiner notes that the Appellant has failed to address dependent claims 2-10,53, and 54 and arguments pertaining to independent claim 1 is representative of claims 1-10,52, and 54.

Claim 11

It is argued by the Appellant that Jacobson fails to disclose "technical controls for implementing the security policy on at least one first computer."

The examiner disagrees with the Appellant's assertion. The technical controls is interpreted in the teachings of Jacobson as being responsible for electronically monitoring network user compliance with a security policy and electronically evaluating policy compliance, undertaking policy compliance action in response to the security policy compliance, see column 2, lines 7-19. Jacobson additionally discloses that hardware implements the policy effectiveness system, or data element as claimed by the Appellant, that includes computers having processors and memories, see column 4, lines 65-67. It is further disclosed by Jacobson that the network communications software programs, or data elements, are used for policy effectiveness and reporting, see column 1, lines 60-63. Jacobson further discloses of block 500 represents the software compliance module of the policy effectiveness system 100, or data element, see column and as shown in Figure 5.

It is argued by the Appellant that Jacobson fails to disclose "enabling creation of a security policy document....by enabling selection of security policies from a set of options."

The examiner respectfully disagrees with the Appellant's assertion. The claimed *security policy document"* is vague as to what constitutes a "security policy document" in the claim language, and there is no language in the claim to further limit the terminology of a "security policy document". It appears that the Appellant is relying upon examples from the specification as to what constitutes a "security policy document" and those elements are not recited in the claim. The teachings of Jacobson disclose of accessing the policy training materials through use of a hypertext list of policy training options that include policy training sessions, review for a policy exam, and taking a policy exam, see column 5, line 66 through column 6, line 4. The presentation through hypertext links is interpreted as the documents that include specific security documents such as policy training sessions, review for a policy exam, and taking a policy exam as is disclosed by Jacobson. Jacobson further discloses that the network policies are generated, or created, by guidelines created from employee feedback obtained during a training session, see column 5, lines 48-50. Block 220 represents a policy training module 105 generating a policy, see column 7, lines 61-62 and as shown in Figure 2. In regards to selection of policies, it is disclosed by Jacobson that the user is presented with a suggested network policy that the organization wishes to implement, see column 5, lines 41-50. The individual and group policy recommendation information is collected and serves as a tool to dictate the creation of the security policy, see column 5, lines 41-50 and column 6, lines 22-26.

The examiner notes that the Appellant has failed to address dependent claims 11-25,55, and 56 and arguments pertaining to independent claim 11 is representative of claims 12-25,55, and 56.

Claims 26 and 51

It is argued Jacobson fails to disclose “a human-readable security policy document” and a “machine readable security policy document containing technical controls” by a computer. It is additionally argued that Jacobson fails to disclose of a "program for creating a security policy document in both human-readable and machine-readable formats".

The examiner disagrees with the Appellant's assertion. Jacobson disclose of presenting information to the user for viewing, or in a "human-readable form", see column 5, lines 37-50. Jacobson further discloses that hardware implements the policy effectiveness system, or software that is in a machine-readable form as claimed by the Appellant, that includes computers having processors and memories, see column 4, lines 65-67. It is further disclosed by Jacobson that the network communications software programs are used for policy effectiveness and reporting, see column 1, lines 60-63. Jacobson further discloses of block 500 represents the software compliance module of the policy effectiveness system 100, or machine readable format, see column and as shown in Figure 5. The technical controls is interpreted in the teachings of Jacobson as being responsible for electronically monitoring network user compliance with a security policy and electronically evaluating policy compliance, undertaking policy compliance action in response to the security policy compliance, see column 2, lines 7-19. Jacobson additionally discloses that hardware implements the policy effectiveness system, or data element as claimed by the Appellant, that includes computers having processors and memories, see column 4, lines 65-67. It is further disclosed by Jacobson that the network communications software programs, or data elements, are used for policy effectiveness and reporting, see column 1, lines 60-63. Jacobson further discloses of block 500 represents the software compliance module of the policy effectiveness system 100, or data element, see column and as shown in Figure 5.

The examiner notes that the Appellant has failed to address dependent claims 27-50 and 53 and arguments pertaining to independent claims 26 and 51 is representative of claims 26-51 and 53.

Claim 16

It is argued by the Appellant that Jacobson fails to disclose of "distributing detect rules".

The examiner disagrees with the Appellant's assertion. The teachings of Jacobson disclose of accessing the policy training materials through use of a hypertext list of policy training options that include policy training sessions, review for a policy exam, and taking a policy exam, see column 5, line 66 through column 6, line 4. The presentation through hypertext links is interpreted as the documents that include specific security documents such as policy training sessions, review for a policy exam, and taking a policy exam as is disclosed by Jacobson. Jacobson further discloses that the network policies are generated, or created, by guidelines created from employee feedback obtained during a training session, see column 5, lines 48-50.

Claims 18 and 19

It is argued by the Appellant that the teachings of Jacobson fail to disclose of *technical controls.*

The examiner disagrees with the Appellant's assertion. The technical controls is interpreted in the teachings of Jacobson as being responsible for electronically monitoring network user compliance with a security policy and electronically evaluating policy compliance, undertaking policy compliance action in response to the security policy compliance, see column 2, lines 7-19.

Claims 53-56

Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Christopher Revak

Primary Examiner 2131

CHRISTOPHER REVAK
PRIMARY EXAMINER

Conferees:

Kambiz Zand KZ

Primary Examiner 2132

Kim Vu KVu

SPE 2135